

# An Attempt to Factor $N = 1002742628021$

Daniel Shanks

June 30, 1978\*

An attempt to factor

$$N = 1002742628021 = [\pi \cdot 10^{15}]/13 \cdot 241$$

by SQUFOF fails but reveals that period of the continued fraction for  $\sqrt{N}$  is relatively short since the queue for SQUFOF contains only the short sequence:

$$751^2, 1165^2, 4, 4, 1165^2, 751^2, 1, \text{ repeat.}$$

The quadratic field  $\mathbf{Q}(\sqrt{N})$  therefore has a relatively large class number  $h$ . The principal period of reduced forms of discriminant  $N$ , not  $4N$ , will be only about  $1/3$  as long since the queue contained 4 and  $N \equiv 5 \pmod{8}$ . Its first form is

$$I = (1, 1001369, -688465)$$

and its form no. 719 is the antisymmetric midform

$$M = (416695, 555161, -416695).$$

Therefore,

$$N = 555161^2 + 416695^2,$$

the period is 1437, and the fundamental unit  $\epsilon$  of  $\mathbf{Q}(\sqrt{N})$  has norm  $-1$ .

The form

$$\begin{aligned} F &= (5, 1001369, -688465/5) \text{ or} \\ &= (5, 1001369, -137693) \end{aligned}$$

clearly has the same discriminant but is inequivalent to  $I$  (and  $M$ ) since the queue did not contain  $5^2$ . This is confirmed by the fact that the period generated by  $F$  has length 1487, not 1437.

We estimate the regulator  $\log \epsilon$  by Levy's Law:

$$\log \epsilon \approx 1487 \cdot \frac{\pi^2}{12 \log 2} = 1766.8,$$

---

\*Hand-written notes..Typed into latex by Stephen McMath in March, 2004

and the Dirichlet function  $L(1, \chi)$  from a partial product of the Euler product:

$$L(1, \chi) \approx \prod_{p=2}^{820} \left( \frac{p}{p - \left(\frac{N}{p}\right)} \right) = .81331.$$

Since

$$h = L(1, \chi) \sqrt{N} / 2 \log \epsilon,$$

we estimate

$$h \approx 230.5;$$

call it 231. The form

$$G = (7, 1001363, -5275091)$$

of discriminant  $N$  is inequivalent to both  $F$  and  $I$  since its period is 1501, which, with Levy's Law, would give  $h \approx 228.7$  instead.

Now, by composition,

$$F^{231} = (-214201, 637141, 696535)$$

and its period 1499 shows that it is inequivalent to  $I, F$ , and  $G$ . But its form no. 746 (nearly half-way around) is

$$(15625, 988039, -424345) = F^6,$$

and therefore  $F^{225} = F^{231-6}$  is equivalent to  $I$ .

However,

$$F^{25} = (-516251, 845063, 139763)$$

is already equivalent to  $I$  since the zigzag diagram of its period begins

$$\begin{array}{r} -516251 \\ \quad 845063 \\ \qquad 139763 \\ \qquad 832093 \\ -555161 \\ \quad 278229 \\ \qquad 416695 \\ \qquad 555161 \\ -416695 \end{array}$$

and its form no. 4 is  $M$ . Therefore,  $F^{25}$  is form no. 716 in the principal period (Since  $F^{25}$  is close to  $M$ ,  $F^{225} = (F^{25})^9$  must also be close to  $M$ , the midform. This explains why  $F^6$  was about half-way around the period of  $F^{231}$ .)

But  $F^5$  is not equivalent to  $I$  since it does not represent  $5^5 = 3125$ . Therefore  $F$  is of order 25 and 25 divides  $h$ . Probably,  $h = 225$ . We confirm this with

$$G^{75} = (-91825, 835889, 827749)$$

which is inequivalent to  $I$  since  $I$  does not represent  $-91825$ . (also, the period of  $G^{75}$  is 1491, not 1437.) But

$$G^{225} = (-279979, 445411, 718225)$$

is equivalent to  $I$  since its negative

$$(279979, 445411, -718225)$$

is form no. 559 in the principal period and therefore  $G^{225}$  is form no.  $1996 = 559 + 1437$ .

So  $h = 225$ , and, since the norm of  $\epsilon$  is  $-1$ ,  $N$  equals  $p^{2k+1}$  for some odd prime  $p$ . But  $k > 0$  is impossible for this  $N$  and so  $N$  is the prime  $p$ .